Rationale for the Selection of the OMAC Variation of XCBC

The National Institute of Standards and Technology (NIST) is developing a block cipher mode of operation for message authentication. From the authentication modes that were submitted to NIST for consideration, NIST initially selected the RMAC algorithm and specified it in the draft NIST Special Publication 800-38B [NIST1]. In response to public comments on the draft, NIST posted a consultation paper [NIST2] that proposed a revision of the draft that focuses on the EMAC construction that underlies RMAC. The public comments and the consultation paper are available at http://www.nist.gov/modes/. In response to further public input, NIST has decided to replace RMAC and EMAC altogether with the OMAC variation of the XCBC algorithm. Among the submitted variations of XCBC, NIST chose OMAC because it appears to offer the best combination of performance characteristics, as discussed at length in [Iw]; the variations are equivalent in security assurance.

This note supplements the technical summary of RMAC, EMAC, and XCBC in [NIST2]. The efficiency evaluation of the algorithms is essentially unchanged, but the security evaluation for XCBC and its variations has changed in light of the improved security bounds that the OMAC submitters provided in [IK]. According to [IK], XCBC and its variations provide proof bounds that are similar to EMAC's. The following is a summary of the security assurance of XCBC and its variations for AES and TDES:

- With AES, an attacker's advantage in the model of the proof would be extremely small for almost any practical number of oracle queries. Nevertheless, because the XCBC submitters reported in [BR] that the security bounds for XCBC are tight, NIST intends to include guidance in the specification on the number of message blocks that a given key may protect.

- With TDES, the new XCBC proof bounds provide some security assurance for general applications. Although this level of assurance may not be sufficient for many modern applications, this deficiency is essentially a consequence of the 64-bit block size of TDES, which is best addressed by migration to AES.

NIST does not know of any security concern that would preclude the selection of RMAC or EMAC, and RMAC arguably offers far greater security assurance with AES than XCBC and its variations on the basis of its security bounds. However, in addition to the new concern discussed in [Iw] and the concerns cited in [NIST2] about the assumptions in the RMAC proof model, RMAC's additional security assurance compared to that of XCBC and its variations is probably not of practical significance for most applications.

EMAC is an internationally standardized algorithm and hence is better established than XCBC and its variations. However, NIST decided that it was more important to take advantage of the opportunity to recommend the best available technology as the AES becomes established. The OMAC variation of XCBC provides better performance characteristics than EMAC with apparently similar security assurance.

NIST already published a draft of RMAC and then a proposal to focus the draft on EMAC, so there may be costs associated with the switch to the OMAC variation of XCBC. However, any costs are expected to be short-term, while the authentication mode is expected to have a long, productive life. Moreover, NIST values the integrity of the public comment process, even when it leads to unexpected delays.

NIST welcomes public comments on the selection of the XCBC algorithm, especially the OMAC variation, in advance of the formal public comment period for the upcoming draft of SP800-38B. Comments may be submitted to EncryptionModes@nist.gov.

References

[BR] J. Black, P. Rogaway, "CBC MACs for arbitrary-length messages: The three key constructions." *Advances in Cryptology---CRYPTO 2000*, pp.197-215, Springer-Verlag, 2000.

Available through http://www.nist.gov/modes/:

[NIST1] Draft NIST Special Publication 800-38B, "Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode."

[NIST2] NIST, "Consultation Paper on the Selection of a Block Cipher Based MAC Algorithm."

[IK] T. Iwata and K. Kurosawa, "Stronger Security Bounds for OMAC, TMAC, and XCBC."

[Iw] T. Iwata, "Comparison of CBC MAC Variants and Comments on NIST's Consultation Paper."